P/4683-7
V14083

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re Application of:	Confirmation No.: 7906
Ralph F. Kalies	Date: December 7, 2009
Serial No.: 10/681,954	Group Art Unit: 3626
Filed: October 8, 2003	Examiner: Reginald R. Reyes

For: METHOD FOR STORING AND REPORTING PHARMACY DATA

VIA EFS-WEB
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R. §41.37

Sir:

This appeal is taken from the Final Office Action mailed April 9, 2009. The Notice of Appeal was filed on October 6, 2009.

I. REAL PARTY IN INTEREST:

The real party in interest in the above-identified application is: Omnicare, Inc.

II. RELATED APPEALS AND INTERFERENCES:

There are no related appeals or interferences of which applicant is aware regarding the above-identified application.

III. STATUS OF CLAIMS:

Claims 1-9 and 15-16 are pending and are involved in the instant appeal.

The Final Office Action rejecting these claims was issued on April 9, 2009. An after-final Amendment was filed on August 24, 2009 canceling claim 10 so as to reduce the issues on appeal. An Advisory Action continuing to reject the claims was mailed on September 28, 2009.

The Notice of Appeal was filed on October 6, 2009.

Claim 10 was rejected under 35 U.S.C. §112. In the after-final Amendment, claim 10 was canceled so the §112 issue is no longer part of this appeal.[1]

Claims 1-10 and 15-16 were finally rejected under 35 U.S.C. §103 as being unpatentable over Donoho et al. U.S. 7,346,655 in view of Schoenberg U.S. 6,463,417.

IV. STATUS OF AMENDMENTS:

A first Office Action was issued on September 9, 2008 rejecting claims 1-14.

An Amendment was filed on January 9, 2009.

The Final Office Action was mailed on April 9, 2009 and an after-final Amendment was filed on August 24, 2009.

An Advisory Action was issued on September 28, 2009. A Notice of Appeal was filed on October 6, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

Independent claim 1 claims a method for storing and reporting pharmacy data. The pharmacy data may comprise patient demographic information, transaction records and prescription information. Specification, paragraph [0018]. The method comprises the step of generating by a plurality of pharmacies 12, electronic pharmacy data 18 comprising medical, financial and transactional information related to pharmaceutical transactions and wherein each of the pharmacies 12 operate within a managed care organization (MCO). Specification, paragraphs [0017]-[0021].

The method further comprises receiving over a network 30 by a processing center 20 of the managed care organization, a data transfer request to transfer respective electronic pharmacy data from at least one of the plurality of pharmacies 12 to the processing center 20. The method

[1] If claim 10 was not properly canceled in the after-final Amendment, it has been canceled on this Appeal.

further comprises providing first access security by the processing center in response to the data transfer request wherein the first access security includes checking credentials defined by the processing center and submitted for authorization by the at least one pharmacy. See specification, paragraph [0026]. In particular, this first access security is provided by the access security screen 40 (Fig. 3).

The method further comprises providing second access security by the processing center in case the at least one pharmacy passes the first access security wherein the second access security includes, prior to accepting the respective electronic pharmacy data by the processing center, checking whether the respective electronic pharmacy meet at least one predefined validity requirement defined by the processing center. As discussed in paragraph [0026] of the specification, if a proper user name and/or password are received for the purpose of transferring data from pharmacy to a processing center 20, access security screen 40 is used to review or check any incoming data before accepting the transfer. Example data checks include validation of the data source, a data format validity check and an optional check for computer viruses. If the data are unacceptable, the transfer is rejected and the pharmacy 12 submitting the data is notified of the rejection via communication portion 45.

The method further comprises receiving, by the processing center, a transfer 18 (Fig. 1) of the respective pharmacy data pursuant to compliance with the second access security. See specification paragraph [0026]. Thus, there is control and security for the inflow of data from the pharmacy to the processing center.

The method further comprises organizing and structuring the electronic pharmacy data by the processing center to format the electronic pharmacy data in accordance with at least one of a predetermined protocol and format, storing the processed electronic pharmacy data in a data warehouse 50, storing subsets of the processed electronic pharmacy data in a datamart 70, the subsets being adapted to meet specific demands of particular requestors in terms of analysis, content, presentation and ease of use thereby to allow preparation of predetermined sets of reports pertinent to the particular requestor. See specification, paragraphs [0028]-[0033].

The method further comprises receiving by the processing center a data request (data extraction) from a data requestor to obtain at least a portion of the processed electronic pharmacy data, the data requestor having a privilege level identifying the type of data available to the requestor (specification, paragraphs [0033]-[0036]), providing third access security by the processing center in response to the data request wherein the third access security includes checking credentials defined by the processing center and submitted for authorization by the data requestor. See specification, paragraph [0032]. In addition to controlling the inflow of data as previously discussed (see "Pharmacy Data Flow" of Fig. 3), access screen 40 screens requests for data extraction from processing center 20. In the embodiment of Fig. 3, access to the data is preferably limited to a predetermined hierarchical group of personnel such as personnel at corporate pharmacies 12, personnel at the regional 14 level and corporate 16 level personnel. In the non-hierarchical embodiment of Fig. 4, access may be limited to a predetermined group of users 26.

The method further comprises providing fourth access security by the processing center in case the data requestor passes the third access security, wherein the fourth access security includes checking whether requested electronic pharmacy data is consistent with the scope of the privilege level of the data requestor. See paragraphs [0033], [0035], security level screen 80. The choices of reports and/or data presented to the requestor for selection may vary with the privileges of the requestor. In this embodiment, the display of choices presented to a requestor on a computer display includes only choices within the particular requestor's scope of privilege.

The method further comprises formatting the portion of the electronic pharmacy data requested by the data requestor into a report pursuant to compliance with the fourth access security, a portion of the electronic pharmacy data for the report being developed from the data in the data warehouse 50 or the subsets of the data in the datamart 70 and further comprising providing the report to the requestor.

Claim 2 recites that the method further comprises the steps of encrypting the pharmacy data before transferring the electronic pharmacy data to the processing center and decrypting (100) the electronic pharmacy data by the processing center after the electronic pharmacy data is received.

Claim 3 recites that the electronic pharmacy data are received by an electronic communications network (30).

Claim 4 recites that the requestor requests and receives the report by means of an electronic communications network (30).

Claim 5 recites that the electronic communications network is an intranet.

Claim 6 recites that the electronic communications network is an Internet.

Claim 7 recites that the requestor is selectively allowed access to a greater or lesser portion of the electronic pharmacy data based upon predetermined criteria. Paragraphs [0033]-[0036].

Claim 8 recites that the method further provides the step of checking the electronic pharmacy data for defects before storing it. (Validation, paragraph [0026]).

Claim 9 recites that the method further comprises the step of encrypting (105) the report of the processing center before sending it to the requestor.

Claim 10 has been canceled.

Claim 15 recites that the report represents financial performance by an individual pharmacy, financial performance by a plurality of pharmacies or a medication review and claim 16 recites that the processing center formats (90) electronic pharmacy data or the report to comply with HIPAA.

Accordingly, the invention relates to a comprehensive system for transferring pharmacy data between pharmacies and the processing center (data inflow) with dual degrees of security for the data flow between pharmacy and processing center to ensure 1) the data provider is authorized and 2) the data is valid; and

for transferring the stored and processed data at the processing center to the pharmacy (data extraction) with two degrees of security to:

1) establish that the requestor is authorized to receive the data; and

2) has the proper privilege level to receive the data.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

The following grounds of rejection are presented for review:

The only remaining rejection is the rejection of claims 1-9 (claim 10 having been canceled) and claims 15-16 under 35 U.S.C. §103 as being unpatentable over Donoho et al. U.S. 7,346,655 in view of Schoenberg U.S. 6,463,417.

VII. ARGUMENT:

It is respectfully submitted that the Examiner's rejection of claims 1-9 and 15-16 under 35 U.S.C. §103 as being unpatentable over Donoho et al. in view of Schoenberg should be reversed.

The Examiner's primary reference is Donoho. Donoho describes a method and apparatus whereby a collection of computers and associated communications infrastructure operate according to a communications process. This process allows information providers to broadcast information to a population of information consumers. The information may be targeted to those consumers who have a precisely formulated need for the information. This targeting may be based on information which is inaccessible to other communication protocols for example, under other protocols, the targeting requires each potential recipient to reveal sensitive information because under other protocols, the targeting requires each potential recipient to reveal information obtainable only after extensive calculations using data available only upon intimate knowledge of the consumer computer, its contents and local environment.

According to the Examiner, Donoho teaches a method for storing and reporting pharmacy data comprising the steps of generating by a plurality of pharmacies (see Donoho, column 53, lines 4-6 and column 92, lines 25-39), each of the pharmacies operating within a managed care organization, electronic pharmacy data comprising medical, financial and transactional information related to pharmaceutical transactions. The Examiner points to column 53, lines 4-6 and column 92, lines 25-39.

The Examiner asserts that Donoho teaches providing a report to a requestor. The Examiner refers to column 53, lines 5-6 and column 53, lines 17-20. The Examiner asserts that Donoho teaches receiving over a network by a processing center of a managed care organization a data transfer request to transfer respective electronic pharmacy data from at least one of the plurality of pharmacies.

The Examiner concedes that Donoho does not teach the remaining elements of Applicant's claim 1, in particular starting with providing the first and second access securities. However, the Examiner asserts that Schoenberg teaches all remaining steps of Applicant's claim 1 including providing the first and second access security, the step of receiving the transfer of the respective electronic pharmacy data, organizing and structuring the electronic pharmacy data and storing the processed electronic pharmacy data in a data warehouse including subsets of the electronic pharmacy data.

The Examiner further asserts that Schoenberg teaches receiving a data request from a data requestor and providing the third and fourth access security, formatting the portion of the electronic pharmacy data requested by the data requestor and providing the report to the requestor.

The Examiner's contentions are without merit. Before addressing the Examiner's arguments, the present invention relates to a method for storing and reporting pharmacy data. The pharmacy data is generated by a pharmacy and is received at the processing center after first and second access security checks. The first access security check determines that the pharmacy submitting the data has the proper credentials. The second access security check determines that the data itself meets at least one predefined validity requirement defined by the processing center. Thus, according to the invention, both the credentials of the sending pharmacy and the validity of the data sent are checked before the data is stored and processed.

Assuming that the data meets the first and second access security, it is processed, organized, structured and stored in the data warehouse.

The second aspect of the Applicant's invention is that once a data request is received to request data from the data warehouse, there are third and fourth access securities. The third access security checks the credentials of the requestor, i.e., whether the requestor is authorized. The fourth access security checks the privilege level of the data requestor so that only data consistent with the requestor's privilege level is allowed to be submitted to the requestor.

Thereafter a report is provided based upon the requestor's privilege level.

The Examiner relies on the Schoenberg reference for the teachings of the first, second, third and fourth access security. However, the Examiner is mistaken about Schoenberg. Schoenberg discloses a system for distributing health information. The Examiner asserts that Schoenberg teaches first and second access security. However, the Examiner is incorrect. Schoenberg does describe certain forms of access security, but they are not the access security as claimed. In column 6, lines 26-50 with reference to Figs. 2 and 3, Schoenberg receives health information and generates security access codes 202, (see Fig. 2) and assigns one or more security access codes to each of the categories of health information. However, Schoenberg does not teach or suggest what Applicant's invention does. Applicant's invention will receive and process the information from the pharmacies if it passes the first and second access security. In contrast, in the Schoenberg reference, there is no provision for determining whether the information that is received is reliable and whether it should be received and processed in the first place, i.e., there is nothing in Schoenberg which teaches or suggests passing first and second access securities before the information is received and processed. Schoenberg merely receives the information and then categorizes it and assigns access codes to it so that if a request is later made for that information, the request will only be granted if the access codes are met.

Schoenberg requires access codes to retrieve the information from the system as requested by a data requestor. Schoenberg does not teach or suggest verifying the information in the first place before it is stored in the system for later retrieval. Thus, Schoenberg fails to teach or suggest providing first access security by the processing center in response to the data transfer request, wherein the first access security includes checking credentials defined by the processing center and submitted for authorization by the at least one pharmacy. The Examiner has confused the "data transfer in" portion for the "data transfer out" portion, i.e., Schoenberg does not teach or suggest providing first access security for receiving information. Schoenberg merely teaches assigning security codes and then when a request for data transfer ("transfer out") is made, checking to see that the user provides the previously provided access code. Thus, at most, Schoenberg may suggest the third access security step of the claims, that is, checking credentials submitted for authorization by the data requestor. However, Schoenberg suggests nothing about providing first access security in order to determine whether the provider of the information is entitled to provide the information in the first place. Furthermore, Schoenberg does not teach or suggest the second access security step which relates to checking the validity of the data itself presented by the data provider. According to the present invention, prior to accepting the respective pharmacy data by the processing center, the data is checked to determine whether it meets at least one predefined validity requirement defined by the processing center. Schoenberg utterly fails to teach or suggest the second access security step.

The Examiner makes much of the fact that Schoenberg teaches a tiered security access as shown in Figs. 2-3 and discussed in column 3, lines 20-52, i.e., that the provider of the information can provide high levels of security for data that it wishes to secure at a higher level. The Examiner is again confusing the security access when data is retrieved from the system with the security access also provided by the present invention for providing data to the system. According to the present invention, the provider of the data is checked to determine if it meets a first access security and the data itself is checked to determine whether it meets a second access security, i.e., that it is valid data. There is nothing in Schoenberg that teaches the first and second access security.

The Examiner has asserted in the Advisory Action that Donoho teaches the step of checking that the data meets at least one predefined validity requirement, i.e., the second access security step. The Examiner points to Donoho, column 21, lines 9-16 in particular, for verification of the integrity of the message by computing a functional from the message. The Examiner asserts that this supports the teaching of the first access security step. Further, the Examiner cites Schoenberg, column 6, lines 26-52 and the table at columns 5-6 as teaching the checking of credentials submitted for authorization by the at least one pharmacy.

The checking of credentials such as user names and passwords described in column 6, lines 26-52 and the table in columns 5-6 of Schoenberg relates to the request for data from the system. Thus, according to Schoenberg, the access security codes generated originally by the patient are checked to determine that the requestor of the information is authorized to receive the information. This does not suggest that a first access security step be implemented when the data is received, i.e., whether the data received from the pharmacy should be processed and stored in the first place. Schoenberg relates to the transfer of data out of the system but does not relate to whether the data should be stored in the system in the first place.

The Examiner asserts that Donoho at column 21, lines 9-16, through its description of a digital digest that can be appended to the message for ensuring message integrity, suggests Applicant's claimed second access security. However, taken as a whole, Donoho and Schoenberg do not teach or suggest Applicant's claim 1 which provides for receiving data, checking a first access security and a second access security before storing and processing the data and furthermore, providing a third access security and a fourth access security when a request for the data that is stored is received. Applicant submits that the combination of Donoho and Schoenberg fails to teach or suggest all the steps of Applicant's claim 1. Accordingly, Donoho and Schoenberg, taken together, do not render independent claim 1 obvious and therefore do not render dependent claims 2-9 and 15-16, obvious under 35 U.S.C. §103.

VIII. CONCLUSION:

In view of the above, it is respectfully requested that claims 1-9 and 15-16 are patentable over the prior art cited and applied by the Examiner. Accordingly, it is submitted that the Board should reverse the Examiner's rejection of the claims.

Applicant reserves the right to request an oral hearing upon receipt of the Examiner's Answer.

Credit card payment for the required filing fee in the amount of $540.00 (large entity) is submitted herewith via EFS-WEB.

If this Appeal Brief is filed after a shortened statutory time period has elapsed and no separate Petition is enclosed, the Commissioner of Patents and Trademarks is petitioned, under 37 C.F.R. §1.136(a), to extend the time for filing a response to the outstanding Office Action by the number of months which will avoid abandonment under 37 C.F.R. §1.135. The fee under 37 C.F.R. §1.17 should be charged to our Deposit Account No. 15-0700.

In the event the actual fee is greater than the payment submitted or is inadvertently not enclosed or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 15-0700.

THIS CORRESPONDENCE IS BEING
SUBMITTED ELECTRONICALLY THROUGH
THE PATENT AND TRADEMARK OFFICE EFS
FILING SYSTEM ON December 7, 2009

Respectfully submitted,

Louis C. Dujmich
Registration No.: 30,625
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

LCD:jh

CLAIMS APPENDIX

1. A method for storing and reporting pharmacy data, comprising the steps of:

generating by a plurality of pharmacies, each of the pharmacies operating within a managed care organization, electronic pharmacy data comprising medical, financial and transactional information related to pharmaceutical transactions;

receiving over a network, by a processing center of the managed care organization, a data transfer request to transfer respective electronic pharmacy data from at least one of the plurality of pharmacies;

providing first access security by the processing center in response to the data transfer request, wherein the first access security includes checking credentials defined by the processing center and submitted for authorization by the at least one pharmacy;

providing second access security by the processing center in case the at least one pharmacy passes the first access security, wherein the second access security includes, prior to accepting the respective electronic pharmacy data by the processing center, checking whether the respective electronic pharmacy data meet at least one predefined validity requirement defined by the processing center;

receiving, by the processing center, a transfer of the respective electronic pharmacy data pursuant to compliance with the second access security;

processing, organizing and structuring the electronic pharmacy data by the processing center to format the electronic pharmacy data in accordance with at least one of a predetermined protocol and format;

storing the processed electronic pharmacy data in a data warehouse;

storing subsets of the processed electronic pharmacy data in a data mart, the subsets being adapted to meet specific demands of particular requestors in terms of analysis, content, presentation and ease of use thereby to allow preparation of predetermined sets of reports pertinent to the particular requestors;

receiving by the processing center a data request from a data requestor to obtain at least a portion of the processed electronic pharmacy data, the data requestor having a privilege level identifying the type of data available to the requestor;

providing third access security by the processing center in response to the data request, wherein the third access security includes checking credentials defined by the processing center and submitted for authorization by the data requestor ;

providing fourth access security by the processing center in case the data requestor passes the third access security, wherein the fourth access security includes checking whether requested electronic pharmacy data is consistent with the scope of the privilege level of the data requestor;

formatting the portion of the electronic pharmacy data requested by the data requestor into a report pursuant to compliance with the fourth access security, the portion of the electronic pharmacy data for the report being developed from the data in the data warehouse or the subsets of the data in the data mart; and

providing the report to the requestor.

2. The method of claim 1, further comprising the steps of:

encrypting by the respective plurality of pharmacies the pharmacy data before ~~it~~ transferring the electronic pharmacy data to the processing center; and

decrypting the electronic pharmacy data by the processing center after the electronic pharmacy data is received.

3. The method of claim 1 wherein the electronic pharmacy data are received via an electronic communications network.

4. The method of claim 3, wherein the requestor requests and receives the report by means of an electronic communications network.

5. The method of claim 4 wherein the electronic communications network is an intranet.

6. The method of claim 4 wherein the electronic communications network is the internet.

7. The method of claim 1, wherein the requestor is selectively allowed access to a greater or lesser portion of the electronic pharmacy data based upon predetermined criteria.

8. The method of claim 1, further comprising the step of checking by the processing center the electronic pharmacy data for defects before storing it.

9. The method of claim 1, further comprising the step of encrypting the report by the processing center before sending it to the requestor.

Claims 10-14 (canceled).

15. The method of claim 1, wherein the report represents financial performance by an individual pharmacy, financial performance by a plurality of pharmacies, or a medication review.

16. The method of claim 1, wherein the processing center formats the electronic pharmacy data or the report to comply with HIPAA.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.